KONICA MINOLTA

COUNT ON KONICA MINOLTA

Hard Drive Data Security

Chris Bilello

Director, Business Development

Konica Minolta Business Solutions U.S.A., Inc.

Konica Minolta Security Features

- On April 19, CBS News aired a story that highlighted the public's fear that confidential and private data could be stolen from the hard drive of an MFP
- During that broadcast, a senior executive at Sharp stated that their products' hard drives could be automatically erased by purchasing a $500 security option
- CBS said that the average American does not want to pay for such protection
- At Konica Minolta, we're glad to hear that!

Konica Minolta Security Features

- Konica Minolta's *standard* equipment includes several different ways to protect the data on the bizhub MFP's hard drive

KONICA MINOLTA

COUNT ON KONICA MINOLTA

One Important Statement from the Story is False!

- During the broadcast, the following was heard:

> **“Nearly every digital copier built since 2002 contains a hard drive - like the one on your personal computer - storing an image of every document copied, scanned, or emailed by the machine.”**

- Konica Minolta refutes this statement as completely inaccurate for our MFP technology
- It is misleading and sensationalistic

KONICA MINOLTA

COUNT ON KONICA MINOLTA

Konica Minolta MFPs do NOT store copies of print, scan, fax or copy jobs on the MFP's hard drive

How it Really Works

- Print, scan, copy, and fax jobs are normally processed in the MFP's volatile Random Access Memory (RAM)
- When the MFP is turned off, any remnants of a job processed in RAM are gone forever and cannot be brought back

KONICA MINOLTA

COUNT ON KONICA MINOLTA

What kind of jobs are stored on the Konica Minolta MFP Hard Drive?

- Jobs scanned or printed to the BOX feature
- Think of boxes as electronic folders on a hard drive
  - Scan to Box
    - Public
    - Private
  - Print to Box
    - Public
    - Private
    - Secure Print Box
  - Incoming fax jobs routed to a BOX
- **These functions have to be enabled by MFP Administrators**
- **The device can be programmed to overwrite any documents residing in ANY Box after a certain period of time**
- Users should be trained on these features

Important Fact

- Documents cannot be stored unknowingly or by accident

KONICA MINOLTA

COUNT ON KONICA MINOLTA

How do we protect documents stored in the MFP's HDD?

- Color bizhubs come standard with a hard drive
- An HDD may be required for a black & white system
- The HDD is protected against unauthorized access to its data by the following methods:
  - Automatic Job Overwrite (Temporary Data Overwrite)
  - HDD Encryption
  - HDD Lock Password
  - Automatic Deletion of Jobs Stored in an electronic USER BOX
  - HDD Overwrite (HDD Sanitizing)
- The administrator of the device has the capability and flexibility to turn each function ON or OFF
  - The default setting for each function is OFF

KONICA MINOLTA

COUNT ON KONICA MINOLTA

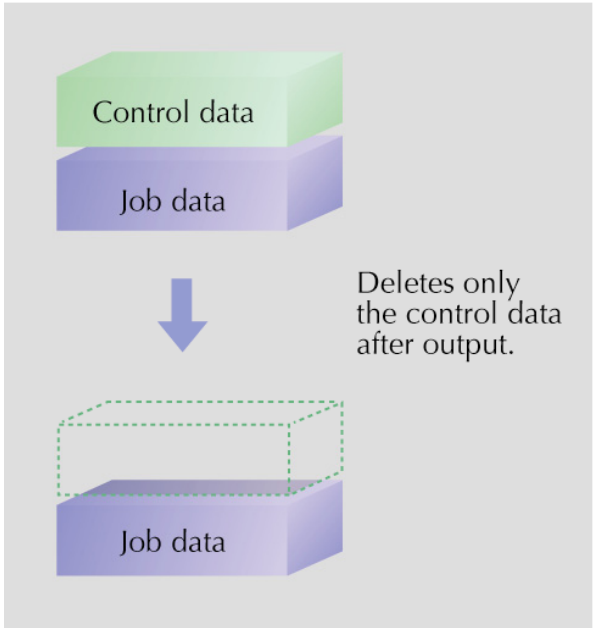
Konica Minolta Hard Drive Data Protection

- **These functions are STANDARD on current and recent models:**
  - Automatic Job Overwrite (Temporary Data Overwrite)
  - HDD Encryption
  - HDD Lock Password
  - Automatic Deletion of Jobs Stored in an electronic HDD BOX
  - HDD Overwrite (HDD Sanitizing)
- Hard Drive Encryption is standard on the current office color line: C220, C280, C360, C452, C552, C652
  - It is an option on the monochrome and previous generation office color MFPs

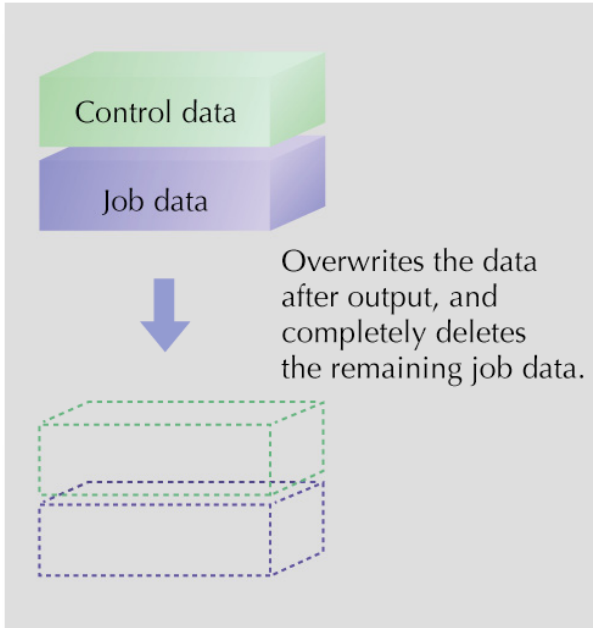
Hard Drive Standard Security Feature

- **HDD Job Overwrite (Temporary Data Overwrite)**
  - The data on the hard drive can be automatically overwritten when:
    - A job is printed out
    - A job is deleted from the User Box

•Ordinary Job Deletion



•bizhub Job Deletion



Job Overwrite (continued)

- **Automatic HDD Job Overwrite (Temporary Data Overwrite)**
  - You can select from 2 modes:
    - Mode 1: Overwrite with 0x00
    - Mode 2 (3 times overwrite):
      - Overwrite with 0x00
      - Overwrite with 0xff
      - Overwrite with the letter “A” (Dx61)
      - Verify
  - These 2 modes support the following standards:
    - US Navy (NAVSO P-5239-26) (Mode 1)
    - Department of Defense (DoD 5220.22-M) (Mode 1)
    - US Air Force (AFSSI5020) (Mode 2)

KONICA MINOLTA

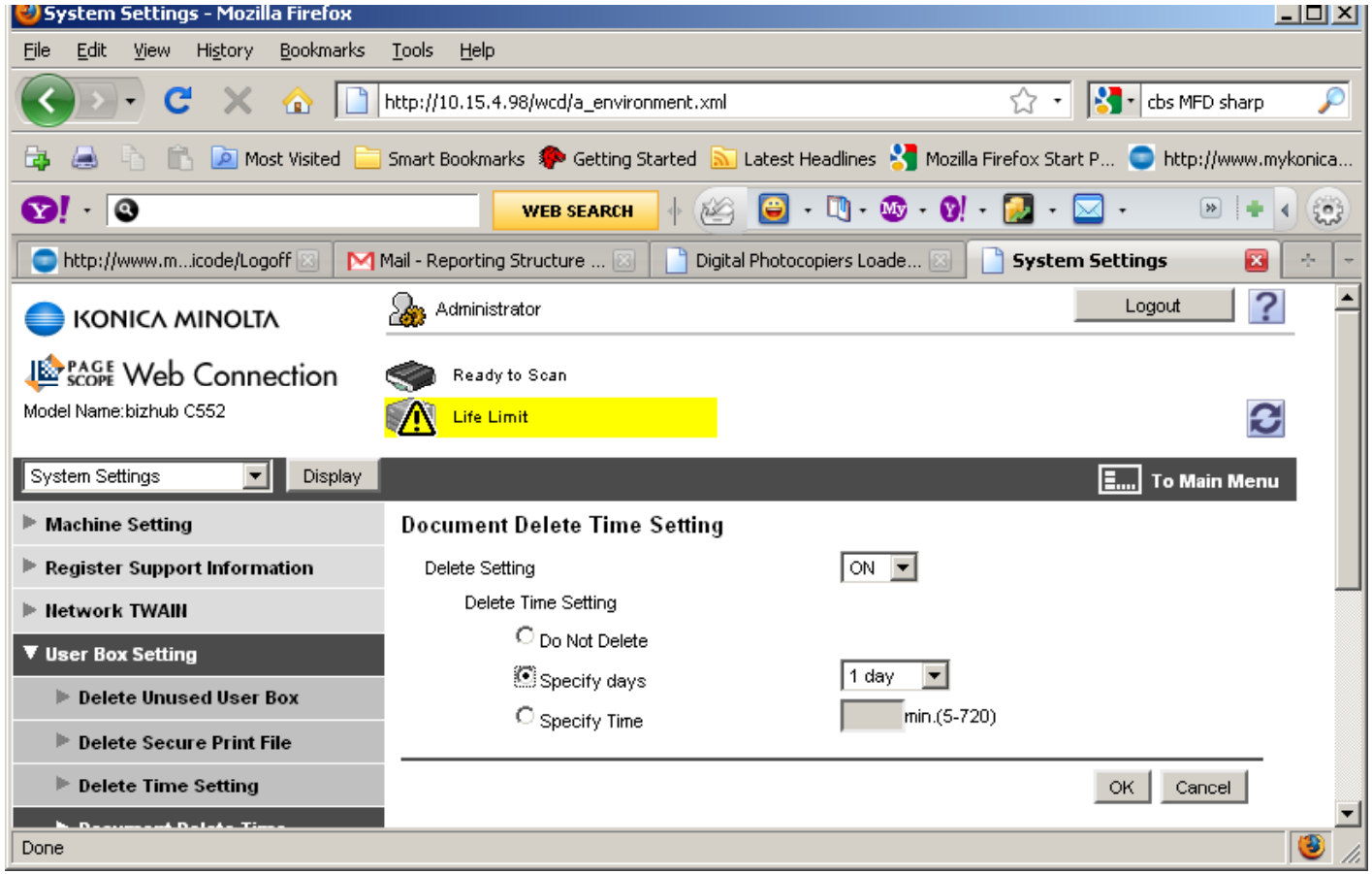
COUNT ON KONICA MINOLTA

Turn ON Automatic Hard Drive Overwrite

KONICA MINOLTA

COUNT ON KONICA MINOLTA

Set Timers for Automatic Document Deletion from the bizhub's Hard Drive



Hard Drive Encryption

- Electronic documents can be stored in a password-protected box on the hard drive
- If an organization is concerned about the security of such data, it can be protected by encrypting it with the HD encryption kit
- The stored data is encrypted using the Advanced Encryption Standard (AES) supporting a 128-bit key
- Once a hard drive is encrypted, its data cannot be read, even if the HDD is removed from the MFP
- Standard on the C220, C280, C360, C452, C552, C652

KONICA MINOLTA

COUNT ON KONICA MINOLTA

Set the Hard Drive Encryption Key

KONICA MINOLTA

More Standard Hard Disk Security

- **HDD Lock Password**
  - It's not easy to remove the hard drive from an MFP, however as an extra precaution…
  - The bizhub hard disk can be locked with a password (20 alphanumeric characters).
  - The lock password makes it impossible to read or access the hard drive's data if the drive is removed from the device and installed on/connected to a computer *or* a different MFP
  - The hard drive is "locked down" and cannot be enabled without the 20 character alphanumeric passcode
  - If someone steals the hard drive from a bizhub MFP:
    - It's a nuisance
    - It's inconvenient
    - Unless they gain access to the password, it's NOT a security threat!

KONICA MINOLTA

COUNT ON KONICA MINOLTA

Lock Down the Hard Drive

Standard HDD Overwrite (HDD Sanitizing)

- Prior to disposal or relocation of a machine, an administrator can overwrite the entire hard disk so that all of its data is *completely* scrubbed

HDD Overwrite (HDD Sanitizing)

- 8 Methods

Mode	Description
Mode 1	Overwrites once with 0x00.
Mode 2	Overwrites with random numbers → random numbers → 0x00.
Mode 3	Overwrites with 0x00 → 0xff → random numbers → verifies.
Mode 4	Overwrites with random numbers → 0x00 → 0xff.
Mode 5	Overwrites with 0x00 → 0xff → 0x00 → 0xff.
Mode 6	Overwrites with 0x00 → 0xff → 0x00 → 0xff → 0x00 → 0xff → random numbers.
Mode 7	Overwrites with 0x00 → 0xff → 0x00 → 0xff → 0x00 → 0xff → 0xaa.
Mode 8	Overwrites with 0x00 → 0xff → 0x00 → 0xff → 0x00 → 0xff → 0xaa → verifies.

KONICA MINOLTA

COUNT ON KONICA MINOLTA

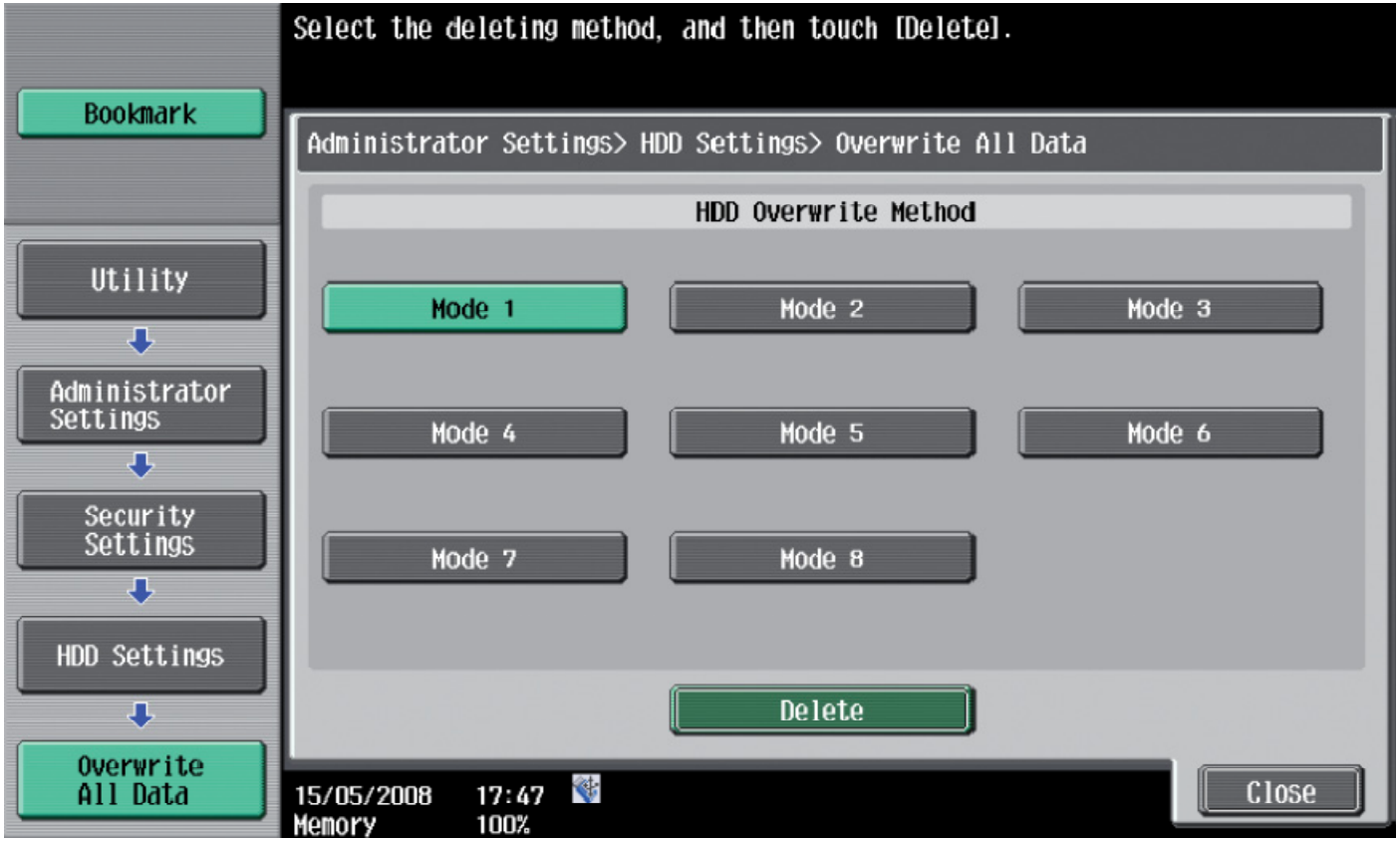
HDD Overwrite (HDD Sanitizing)

- The 8 overwriting methods meet the following standards:
  - Mode 1
    - Japan Electronic and Information Technology Association
    - Russian Standard (GOST)
  - Mode 2
    - Current NSA (National Security Agency) Standard
  - Mode 3
    - National Computer Security Center (NCSC-TG-025)
    - US Navy (NAVSO P-5239-26)
    - Department of Defense (DoD 5220.22-M)
  - Mode 4
    - Army Regulations (AR380-19)
  - Mode 5
    - Former NSA Standard
  - Mode 7
    - German Standard (VISTR)
  - Mode 8
    - US Air Force (AFSSI5020)

KONICA MINOLTA

COUNT ON KONICA MINOLTA

Choose the Hard Drive Sanitize Method



KONICA MINOLTA

COUNT ON KONICA MINOLTA

Current & Recent Models Support

- **Monochrome bizhub**
  - 200, 250, 350
  - 220, 280, 362
  - 360, 420, 500
  - 361, 421, 501
  - 600, 750
  - 601, 751
  - 950, 1051, 1200 (confirmed 8 modes of hard drive sanitization)
- **Color bizhub**
  - C250, C252, C351, C451
  - C203, C253, C300, C353
  - C450, C550, C650
  - C220, C280, C360
  - C452, C552, C652
  - C5501, C6501 (confirmed 8 modes of hard drive sanitization)

Additional Information

- **From the Konica Minolta public web site**
  - http://kmbs.konicaminolta.us/content/products/subcategories/as_security.html
  - Security White Paper
  - BLI Security Report
  - Link to Common Criteria ISO 154080 Documentation
  - Other Security related information
- **Security manuals for bizhub MFP models**
  - http://kmbs.konicaminolta.us/content/support/supportmanuals.html